RELIABILITY | RESILIENCE | SECURITY

POWERING TODAY. PROTECTING TOMORROW.

NERC

2025-06 Project Update

Changes to CIP-010-6 Configuration and Change Management and Vulnerability Assessments and CIP-013-4 Supply Chain Risk Management

(Revisions to current CIP-010-5 and CIP-013-3 under Project 2025-06)

Michelle Johnson, NERC Standards Developer

May 2026

Purpose & Regulatory Basis (FERC Order 912)

Regulatory Basis

In FERC Order 912, the Commission identified gaps in the existing CIP-013-3 standards related to how Responsible Entities identify, reassess, and respond to supply chain cyber risks, including explicit protections for Protected Cyber Assets (PCAs).

Project Objective

Project 2025-06 updates CIP-010-5 and CIP-013-3 to implement the directives in FERC Order 912, while preserving flexibility for each Responsible Entity to design and maintain a supply chain risk management program and configuration and change management and vulnerability assessments appropriate to its individual risk profile and operating environment.

Scope of Revisions

The proposed modifications focus on strengthening risk identification and reassessment, documenting defensible risk-based decisions, and extending appropriate protections to PCAs.

- Per footnote 2 of FERC Order 912, the Commission directed that PCAs be included within CIP-005-8 and CIP-010-5 (current as of 04/01/2026).
- CIP-005-8 already includes PCAs and does not require modification.
- CIP-010-5 will require conforming updates to reflect PCA inclusion in Part 1.3.

Priority and Direction

This is a FERC-directed, high-priority project with a required completion date of May 21, 2027.

Status, Next Steps & Industry Engagement

Current Status

- Ballot package sent to the May 21st SC for approval to go to ballot.
- Targeted industry outreach is underway now and will continue through the ballot period.

What's Next

- 45-day comment and ballot period, targeting May 26 to July 9th.

Continued Outreach & Engagement

- The Drafting Team will continue targeted outreach to validate draft direction, and address concerns early which should reduce downstream issues during balloting.

What We Need From You

- Feedback on clarity and auditability of the draft requirements, practical implementation considerations, and impacts to existing supply chain risk management processes.

FERC Order 912 Directives

FERC ORDER 912 Directives
fn2. In this notice of proposed rulemaking, the term SCRM Reliability Standards includes Reliability Standards CIP-005-7 (Electronic Security Perimeter(s)), CIP-010-4 (Configuration Change Management and Vulnerability Assessments), and CIP-013-2 (Supply Chain Risk Management).
p. 26 Standards that would establish specific timing requirements for a responsible entity to evaluate its equipment and vendors to better identify supply chain risks; NERC should establish (1) a maximum time frame between when an entity performs its initial risk assessment during the procurement process and when it installs the equipment and (2) periodic requirements for an entity to reassess the risk associated with vendors, products, and services procured under any contracts for supply chain risks that may have developed or changed since the contract commenced.
p. 29 Clarify that the directive here already includes reassessment of spare equipment and emergency repairs.
p. 32 that establish a maximum time frame between when a responsible entity performs its initial vendor and equipment risk assessment during the procurement process and when it deploys the equipment. If a responsible entity does not deploy the equipment or software within the specified time limit, the new or modified Reliability Standards should require responsible entities to perform an updated risk assessment prior to deployment.
p. 53 require responsible entities to establish a process to document, track, and respond to all identified supply chain risks; that existing SCRM Reliability Standards are inadequate to ensure consistent, timely, and appropriately documented responses to identified vendor risks.
p. 63 include PCAs as applicable assets
p. 69 to develop and submit for Commission approval new or modified Reliability Standards within 18 months of the effective date of this rule.

What Is Changing Under CIP-013-4

Shift in focus to include Product-Based Risk Assessments

- CIP-013-4 clarifies that supply chain risk management is also focused on products and services, rather than solely on vendors.
- Risk assessments are performed for specific products, software, and services, including spare equipment and emergency repairs.

Mandatory Risk Reassessments

- CIP-013-4 introduces explicit requirements to reassess supply chain risks, including:
  - Reassessment prior to deployment when prior assessments are no longer current, and
  - Periodic or event-driven post-deployment reassessments when supply chain risks may have changed.

Why This Matters

- These changes ensure supply chain risks are continuously evaluated across the system lifecycle, rather than assessed only at initial procurement.

Substantive Changes (draft as of 4/30/2026)

Updates in BOLD

- **R1.** Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), **Protected Cyber Assets (PCAs),** and Shared Cyber Infrastructure (SCI). The plan(s) shall include: [*Violation Risk Factor: Medium] [**Time Horizon: Long-term Planning** and Operations Planning]*

- One or more process(es) used in planning for the procurement of applicable systems listed in Requirement R1 to identify and assess cyber security risk(s) to the BES from vendor products or services, **including spare equipment and emergency repairs**, resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

- **1.3 One or more process(es) used for performing a risk assessment prior to the deployment of products or services, including spare equipment and emergency repairs, when the period between the most recently completed risk assessment and the deployment exceeds:**
  - **24 calendar months, for the high impact applicable systems listed in R1; or**
  - **36 calendar months, for the medium impact applicable systems listed in R1.**

Substantive Changes (continued)

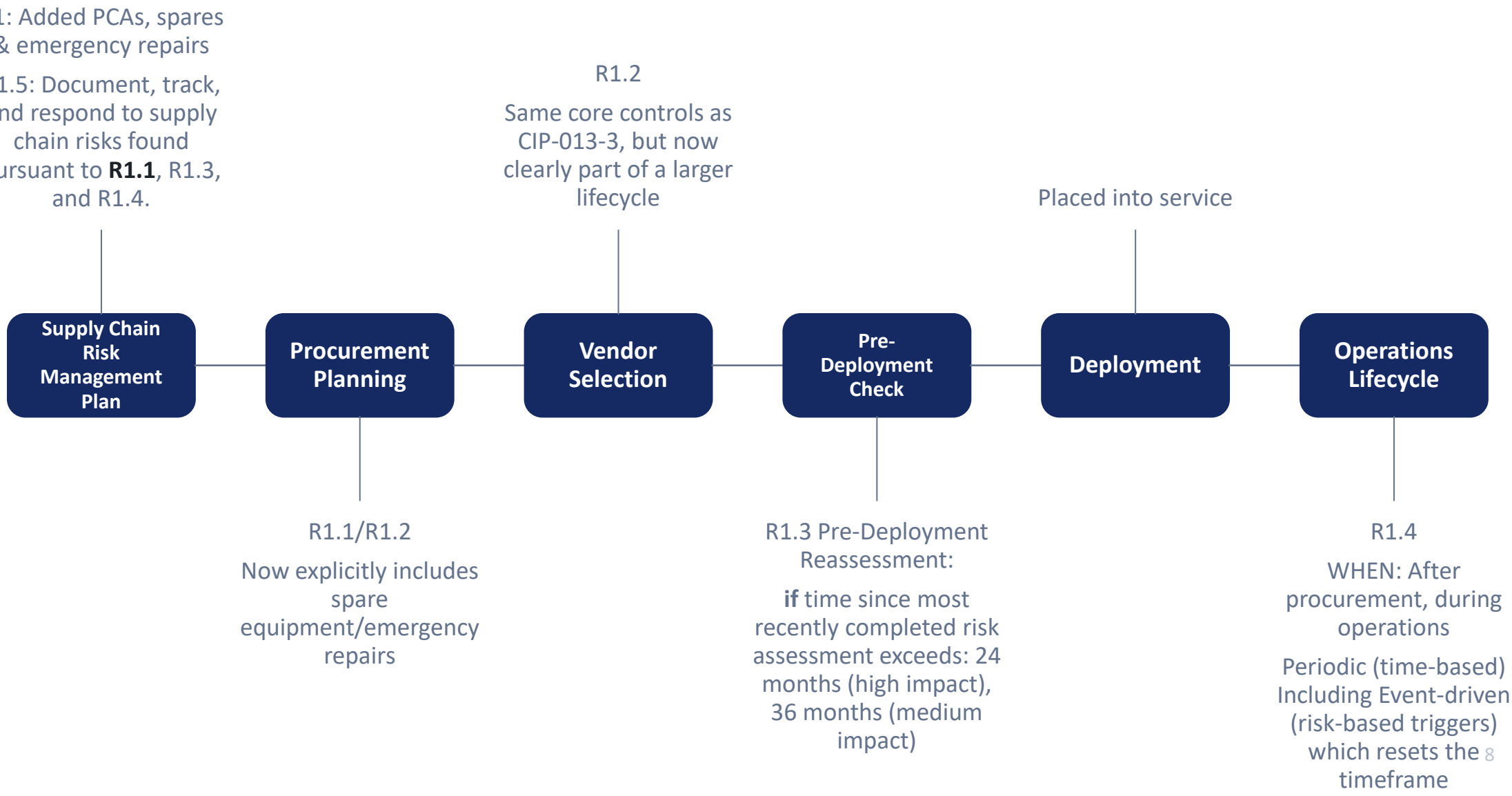
Updates in BOLD

- **1.4 One or more process(es) used to periodically reassess the risk post deployment associated with vendors, and products, or services procured under any contracts for supply chain risks that may have developed or changed since the contract or contractual obligation commenced.**

- **1.5 One or more process(es) used to document, track, and respond to supply chain risks identified through the execution of the risk assessments performed pursuant to R1.1, R1.3, and R1.4.**

- R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium]* ***[Time Horizon: Long-term Planning*** *and Operations Planning]*

Draft CIP-013-4 Changes by Lifecycle Stage



VSL Changes and Implementation Plan

Violation Severity Level (VSL) Updates

- VSLs were reviewed and updated to ensure appropriate differentiation between:
  - Documentation-related deficiencies and
  - Failures to implement required processes
- Implementation failures generally align with higher VSLs than documentation-only issues, consistent with NERC VRF/VSL criteria, and FERC VSL Guidelines Issues

Reliability Standard CIP-010-6 and CIP-013-04

- The standard shall become effective on the first day of the first calendar quarter that is eighteen *(18)* months after approval of the standard.

Performance Expectations

- CIP-013-4 Part 1.3 and Part 1.4 risk assessments are not required prior to the effective date of the standard
- Protected Cyber Assets (PCAs) procured prior to the effective date do not require a Part 1.1 supply chain risk assessment under CIP-013-4

NERC

Discussion

Point of Contact

- Point of contact
  - Michelle Johnson, NERC Standards Developer
  - Michelle.Johnson@nerc.net